

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

Zaal Panthaki and Alexander Crous, on behalf
of themselves and all others similarly situated,

Plaintiffs,

v.

COINBASE GLOBAL, INC.
and COINBASE, INC.

Defendants.

Case No. 1:25-cv-04094

CLASS ACTION

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiffs Zaal Panthaki and Alexander Crous (“Plaintiffs”), on behalf of themselves and all others similarly situated, bring this Class Action Complaint (the “Action”) against the above-captioned Defendants, Coinbase Global, Inc. and its subsidiary Coinbase, Inc. (collectively, “Coinbase” or “Defendants”), and allege upon personal knowledge as to themselves and their own actions, and upon information and belief as to all other matters, as follows:

I. NATURE OF THE ACTION

1. Plaintiffs bring this class action against Coinbase for its failure to secure and safeguard personally identifiable information of millions of former and current Coinbase customers.

2. On May 15, 2025, Coinbase announced via an 8-K filing with the United States Securities and Exchange Commission (“SEC”) that an unnamed threat actor claimed (via a May

11, 2025 email) to have obtained information regarding Coinbase customers, names, addresses, phone numbers, email addresses, last four digits of social security numbers, Coinbase account information, bank account information, governmental-ID images, and account data, among other personal information (collectively, the “PII”).

3. Coinbase, as a substantial business, had the resources to take seriously the obligation to protect private information. However, Coinbase failed to invest the resources necessary to protect the PII of Plaintiffs and Class members.

4. The actions of Coinbase related to this Data Breach are unconscionable. Upon information and belief, Coinbase failed to implement practices and systems to mitigate against the risks posed by Coinbase’s negligent (if not reckless) IT practices. As a result of these failures, Plaintiffs and Class members face a litany of harms that accompany data breaches of this magnitude and severity.

5. As such, Plaintiffs, on behalf of themselves and all others similarly situated, bring this Action for restitution, actual damages, nominal damages, statutory damages, injunctive relief, disgorgement of profits and all other relief that this Court deems just and proper.

II. JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005 (“CAFA”), 28 U.S.C. § 1332(d). The amount of controversy exceeds the sum or value of \$5,000,000 exclusive of interests and costs, there are more than 100 putative Class members, and minimal diversity exists because one or more putative Class members are citizens of a different state than Defendants.

7. This Court has personal jurisdiction over Coinbase because it maintains its principal place of business and operations in New York City and because Coinbase intentionally availed itself of this jurisdiction by providing services in New York City.

8. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Coinbase's principal place of business is in New York City, because Coinbase operates extensively in this District and because a substantial part of the events, acts and omissions giving rise to Plaintiffs' claims occurred in this District.

III. PARTIES

Plaintiffs

9. Plaintiff Panthaki is a citizen of the state of Maine. Plaintiff Panthaki is a customer of Coinbase.

10. Plaintiff Crous is a citizen of the state of Texas. Plaintiff Crous is a customer of Coinbase.

Defendant Coinbase

11. Defendant Coinbase Global, Inc. (together with its subsidiary, Coinbase, Inc.) is a major cryptocurrency company with its principal place of business in New York City. Coinbase is one of the world's largest cryptocurrency, providing a platform for investors (and speculators) to purchase, hold, and sell credible cryptocurrencies. Coinbase's principal executive offices are located on New York City's fashionable Madison Avenue, at One Madison Avenue.

IV. FACTUAL ALLEGATIONS

A. Defendants' Businesses and Collection of Private Information

12. In the course of doing business, Coinbase acquires a significant amount of highly sensitive and valuable private information from prospective and current customers, including the acquisition of the PII of Plaintiffs and Class members.

13. As a condition of receiving this PII, Plaintiffs and Class members entrusted that Coinbase would only use their data for business purposes in a manner that was safe and secure.

14. By obtaining, collecting, using, and deriving a benefit from Plaintiffs and Class members' PII, Coinbase assumed legal and equitable duties and knew or should have known that it was responsible for ensuring the safety and security of Plaintiffs and Class members' PII and to protect such PII from unauthorized disclosure and exfiltration.

15. Plaintiffs and Class members relied on Coinbase to keep their PII confidential and only to make authorized disclosures of this PII, which Coinbase failed to do.

B. The Data Breach

16. As noted, on May 11, 2025, a threat actor informed Coinbase that he or she obtained the PII of countless Coinbase customers (the "Data Breach").

17. To illustrate the enormous magnitude of the Data breach, it is notable that, in its May 15, 2025 filing with the SEC, Coinbase stated that it preliminarily estimates that it might incur expenses of between \$180 million and \$400 million relating to remediation and other costs as a result of the Data Breach.

18. Not only do Plaintiffs and Class members have to contend with the harms caused by the Data Breach, but Coinbase's response has been woefully insufficient.

19. On information and belief, the PII compromised in the files accessed by hackers was not encrypted. This can also be inferred given that the hackers were able to access the PII listed above.

20. The removal of PII from Coinbase's systems demonstrates that this cyberattack was targeted due to Coinbase's status as a well-known cryptocurrency business that houses sensitive PII. Armed with this PII, data thieves (as well as downstream purchasers of the stolen PII), can commit a variety of crimes, including: opening new financial accounts in Class members' names, taking out loans in Class members' names, using Class members' information to obtain government benefits, filing fraudulent tax returns using Class members' tax identification information, obtaining driver's licenses in Class members' names but with a different photograph, and giving false information to police during an arrest.

21. Due to Coinbase's flawed security measures and Coinbase's incompetent response to the Data Breach, Plaintiffs and Class members now face a present, substantial, and imminent risk of fraud and identity theft and must deal with that threat forever.

22. Despite widespread knowledge of the dangers of identity theft and fraud associated with cyberattacks and unauthorized disclosure of PII, and despite Coinbase's large operating budget, Coinbase provided unreasonably deficient protections prior to the Data Breach, including but not limited to a lack of security measures for storing and handling PII, as well as inadequate employee training regarding how to access, oversee the protection of, and handle and safeguard this sensitive set of information.

23. Coinbase failed to adequately adopt and train its employees on even the most basic of information security protocols, including storing, locking, encrypting and limiting access to current and former consumers and employees' highly sensitive PII; implementing guidelines for accessing, maintaining, and communicating sensitive PII; and protecting sensitive PII by implementing protocols on how to utilize such information.

24. Coinbase' failures caused the unpermitted disclosure of Plaintiffs' and Class members' PII to an unauthorized third-party cybercriminal and put Plaintiffs and Class members at serious, immediate, and continuous risk of identity theft and fraud.

25. The Data Breach that exposed Plaintiffs' and Class members' PII was caused by Coinbase's violation of its obligations to abide by best practices and industry standards concerning its information security practices and processes.

26. Coinbase, despite being a technologically advanced organization, failed to comply with basic security standards or to implement security measures that could have prevented or mitigated the Data Breach.

27. Coinbase failed to ensure that all personnel with access to its current/former actual and prospective students' PII were properly trained in retrieving, handling, using and distributing sensitive information. This means that personnel are trained to apply relevant updates and software patches, as Coinbase should have done here.

C. The Data Breach Was Foreseeable

28. Coinbase has weighty obligations created by industry standards, common law, and its own promises and representations to keep PII confidential and to protect from unauthorized access and disclosure.

29. Plaintiffs and Class members provided their PII to Coinbase with the reasonable expectation and mutual understanding that Coinbase would comply with its obligations to keep such information confidential and secure from unauthorized access.

30. Coinbase's data security obligations were particularly acute given the substantial increase in ransomware attacks and/or data breaches in various industries – including financial institutions – preceding the date of the Data Breach.

31. Coinbase was aware of the risk of data breaches because such breaches have dominated the headlines in recent years.

32. PII, like the PII targeted by the hackers in this Action, is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used in a variety of unlawful manners. PII can be used to distinguish, identify or trace an individual's identity. This can be accomplished alone or in combination with other personal or identifying information that is connected or linked to an individual, such as the information compromised in the Data Breach.

33. Given the nature of the Data Breach, it is foreseeable that the compromised PII can be used by hackers and cybercriminals in a variety of different ways.

34. Cybercriminals who possess Class members' PII can (in tandem with other information) obtain Class members' tax returns or open fraudulent credit card or other types of accounts in Class members' names.

35. The increase in such attacks, and attendant risk of future attacks, was widely known.

36. As such, this specific Data Breach was foreseeable. Defendants were cognizant of data breaches because of how common and high-profile data breaches have become with respect to consumer-facing businesses, such as Coinbase.

D. Defendants Failed to Follow FTC Guidelines and Industry Standards

37. Experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the data which they collect and maintain. The reason this data is so valuable is because it contains PII, which can be sold and weaponized for purposes of committing various identity theft-related crimes. It is well-known that, because of the value of this data and PII, businesses that collect, store, maintain, and otherwise utilize or profit

from PII must take necessary cybersecurity safeguards to ensure that the data they possess is adequately protected.

38. Government agencies also highlight the importance of cybersecurity practices. For example, the Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices.

39. According to the FTC, the need for data security should be factored into all business decision-making.

40. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses.

41. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network’s vulnerabilities; and implement policies to correct any security problems.

42. The guidelines also recommend that businesses use an intrusion detection system to detect and expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

43. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

44. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, in some cases treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further explicate and clarify the measures businesses must take to meet their data security obligations.

45. Defendants failed to properly implement some or all of these (and other) basic data security practices.

46. Defendants’ failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

47. Defendants at all times were fully aware of obligations to protect PII. Defendants were also keenly aware of the significant repercussions that would result from the failure to do so.

48. Experts studying cyber security routinely identify consumer-facing businesses as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

49. Several best practices have been identified that, at a minimum, should be implemented by consumer-facing businesses such as Coinbase, include but are not limited to: educating all employees about cyber security; requiring strong passwords; maintaining multi-layer security, including firewalls, anti-virus, and anti-malware software; utilizing encryption; making data unreadable without a key; implementing multi-factor authentication; backing up data; and limiting which particular employees can access sensitive data.

50. Other best cybersecurity practices that are standard in the industry include installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; and training staff regarding critical points.

51. These foregoing frameworks are existing and applicable industry standards. Coinbase failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

E. Defendants' Breaches of Their Obligations

52. Defendants breached their obligations to Plaintiffs and Class members and were otherwise negligent and/or reckless because Defendant failed to properly maintain, oversee and safeguard their computer systems, network and data. In addition to their obligations under federal and state law, Defendants owed a duty to Plaintiffs and Class members to exercise reasonable care when obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed or misused by unauthorized persons. Defendants owed a duty to Plaintiffs and Class members to provide reasonable security, including complying with industry standards and requirements, training for their staff and ensuring that their computer systems, networks, and protocols adequately protected the PII of Plaintiffs and Class members.

53. Defendants' wrongful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

- b. Failing to adequately protect current or former consumers' PII;
- c. Failing to implement updates and patches in a timely manner;
- d. Failing to properly monitor third-party data security systems for existing intrusions, brute-force attempts and clearing of event logs;
- e. Failing to ensure that all employees and third-parties apply all available and necessary security updates;
- f. Failing to ensure that all employees and third-parties install the latest software patches, update their firewalls, check user account privileges, or ensure proper security practices;
- g. Failing to ensure that all employees and third-parties practice the principle of least-privilege and maintain credential hygiene; and failing to avoid the use of domain-wide, admin-level service accounts;
- h. Failing to adequately oversee employees and third-party vendors;
- i. Failing to ensure that all employees and third-parties employ or enforce the use of strong randomized, just-in-time local administrator passwords; and
- j. Failing to properly train and supervise employees and third-parties in the proper handling of inbound emails.

54. As the result of allowing their computer systems to fall into dire need of security upgrading and its inadequate procedures for handling cybersecurity threats, Coinbase negligently and wrongfully failed to safeguard Plaintiffs' and Class members' PII.

55. Accordingly, as further detailed herein, Plaintiffs and Class members now face a substantial, increased, and immediate risk of fraud, identity theft, and the disclosure of their most sensitive and deeply personal information.

F. Data Breaches Are Harmful and Disruptive

56. The United States Government Accountability Office (“GAO”) released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”

57. That is because all victims of a data breach may be exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it because there is (unfortunately) a market for personally identifiable information, like the PII compromised by the Data Breach.

58. Cybercriminals do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims’ identities in order to engage in illegal financial transactions under the victims’ names. Because a person’s identity is akin to a puzzle, the more accurate individual pieces of data an identity thief obtains regarding a person, the easier it is for that thief to take on the victim’s identity, or otherwise harass or track the victim.

59. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as “social engineering” to obtain even more information regarding a victim’s identity, such as a person’s login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

60. Because of the threat of these harms, the FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and potentially obtaining an

extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

61. Theft of PII is gravely serious. PII is an extremely valuable property right.

62. Its value is axiomatic, considering the value of “big data” in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates that PII has considerable market value.

63. According to the GAO:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

64. Private information, such as the PII compromised herein, is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for years. The private information of consumers remains of high value to criminals, as evidenced by the prices paid through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, private information (inclusive of a Social Security number) can be sold at a price from \$40 to \$200, and bank details have a price range of \$50 to \$200. Experian reports that a stolen credit card or debit card number can sell between \$5 to \$110 on the dark web. Clearly, all this data has real value – which is why it is often targeted and stolen in the first place.

65. Because the PII compromised in the Data Breach has been dumped on the dark web, Plaintiffs and Class members are at a substantial imminent risk of injury including an increased risk of fraud and identity theft for many years into the future.

66. Thus, Plaintiffs and Class members must vigilantly monitor their financial accounts and other indices of identity theft (*i.e.*, the mail, email, etc.) for many years to come.

G. Harm to Plaintiffs and the Class

67. Plaintiffs suffered actual injury from having their PII compromised as a result of the Data Breach including, but not limited to (a) misuse of their compromised PII; (b) damage to and diminution in the value of their PII, a form of property that Defendants obtained from Plaintiffs; (c) violation of their privacy, including the compromise of highly sensitive PII; (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud; and (e) actual and potential out-of-pocket losses including the loss of time.

V. CLASS ALLEGATIONS

68. Plaintiffs bring this nationwide class on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure. The “Class” that Plaintiffs seek to represent is defined as follows:

Class Definition. All persons whose PII was maintained by Coinbase which was compromised in the Data Breach.

69. Excluded from the Class are Defendants and Defendants’ subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

70. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

71. **Numerosity**. Media reports indicate that the Data Breach compromised PII of at least many thousands of individuals. Therefore, the members of the Class are so numerous that joinder of all members is impractical.

72. **Commonality**. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

- a. Whether Defendants unlawfully used, maintained, lost or disclosed Plaintiffs' and Class members' PII;
- b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;
- e. Whether Defendants owed a duty to Plaintiffs and Class members to safeguard their PII;
- f. Whether Defendants breached their duties to Plaintiffs and Class members to safeguard their PII;
- g. Whether computer hackers obtained Plaintiffs' and Class members' PII in the Data Breach;
- h. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;
- i. Whether Plaintiffs and Class members suffered legally cognizable damages as a result of Defendants' misconduct;
- j. Whether Defendants' acts, inactions, and practices complained of herein amount to a breach of contract, and/or common law negligence, and whether Defendants have been unjustly enriched;

k. Whether Defendants failed to provide notice of the Data Breach in a timely and proper manner; and

l. Whether Plaintiffs and Class members are entitled to damages, civil penalties, equitable relief and/or injunctive relief.

73. **Typicality.** Plaintiffs' claims are typical of those of other Class members because Plaintiffs' PII, like that of every other Class member, was compromised by the Data Breach. Further, Plaintiffs, like all Class members, were injured by Defendants' uniform conduct. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of other Class members arise from the same operative facts and are based on the same legal theories.

74. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent and protect the interests of the Class in that they have no disabling or disqualifying conflicts of interest that would be antagonistic to those of the other members of the Class. The damages and infringement of rights Plaintiffs suffered are typical of the other Class members, and Plaintiffs seek no relief that is antagonistic or adverse to the members of the Class. Plaintiffs have retained counsel experienced in complex class action litigation, including, but not limited to, data privacy class action litigation, and Plaintiffs intend to prosecute this action vigorously.

75. **Superiority of Class Action.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy, as the pursuit of numerous individual lawsuits would not be economically feasible for individual Class members, and certification as a class action will preserve judicial resources by allowing the Class's common issues to be adjudicated in a single forum, avoiding the need for duplicative hearings and discovery in

individual actions that are based upon an identical set of facts. Without a class action, it is likely that many members of the Class will remain unaware of the claims they may possess.

76. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws and the ascertainable identities of Class members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

77. Adequate notice can be given to Class members directly using information maintained in Defendants' records.

78. **Predominance**. The issues in this action are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Defendants have engaged in a common course of conduct toward Plaintiffs and Class members. The common issues arising from Defendants' conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these issues in a single action has important and desirable advantages of judicial economy.

79. This proposed class action does not present any unique management difficulties.

COUNT I

NEGLIGENCE

80. Plaintiffs repeat and reallege all preceding paragraphs as if fully set forth herein.

81. Coinbase knowingly collected, acquired, stored, and/or maintained Plaintiffs' and Class members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting the PII from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

82. The duty included obligations to take reasonable steps to prevent disclosure of the PII, and to safeguard the information from theft. Coinbase's duties included the responsibility to design, implement, and monitor its and its data security systems, policies, and processes to protect against reasonably foreseeable data breaches such as this Data Breach.

83. Defendants owed a duty of care to Plaintiffs and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, policies, and procedures, and the personnel responsible for them, adequately protected the PII.

84. Defendants owed a duty of care to safeguard the PII due to the foreseeable risk of a data breach and the severe consequences that would result from their failure to so safeguard PII.

85. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and those individuals who entrusted Defendants with their PII, which duty recognized by laws and regulations including but not limited the FTCA as well as common law.

86. In addition, Defendants have a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

87. Defendants' duty to use reasonable care in protecting PII arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect PII that it acquires, maintains, or stores.

88. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Plaintiffs' and Class members' PII, as alleged and discussed above.

89. It was foreseeable that Defendants' failure to use reasonable measures to protect Class members' PII would result in injury to Plaintiffs and Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in consumer-facing industries and universities and colleges.

90. It was therefore foreseeable that the failure to adequately safeguard Class members' PII would result in one or more types of injuries to Class members.

91. The imposition of a duty of care on Defendants to safeguard the PII they maintained, transferred, stored or otherwise used is appropriate because any social utility of Defendants' conduct is outweighed by the injuries suffered by Plaintiffs and Class members as a result of the Data Breach.

92. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class members are at a current and ongoing imminent risk of identity theft, and Plaintiffs and Class members sustained compensatory damages including: (i) invasion of privacy; (ii) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (iii) loss of time and loss of productivity incurred mitigating the material risk and imminent threat of identity theft; (iv) financial "out of pocket" costs incurred due to actual identity theft; (v) loss of time incurred due to actual identity theft; (vi) loss of time due to increased spam and targeted marketing emails; (vii) diminution of value of their PII; (viii) future costs of identity theft monitoring; (ix) anxiety, annoyance and nuisance, and (x) the continued risk to PII, which remains in Defendants' and the threat actor's respective control, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' PII.

93. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

94. Coinbase's negligent conduct is ongoing, in that Coinbase still holds the PII of Plaintiffs and Class Members in an unsafe and unsecure manner.

95. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

COUNT II

BREACH OF IMPLIED CONTRACT

96. Plaintiffs repeat and reallege all preceding paragraphs as if fully set forth herein.

97. Defendants provide services to Plaintiffs and Class members. Defendants formed an implied contract with Plaintiffs and Class members through their conduct.

98. Through Defendants' individual provision of services, it knew or should have known that it must protect Plaintiffs' and Class members' confidential PII in accordance with Defendants' stated policies, practices and the applicable law.

99. As consideration, Plaintiffs and Class members turned over valuable PII in exchange for Coinbase's services.

100. Defendants accepted possession of Plaintiffs' and Class members' PII for the purpose of providing services to Plaintiffs and Class members. In delivering their PII to Defendants, Plaintiffs and Class members intended and understood that Defendants would adequately safeguard the PII as part of the provision or receipt of those services.

101. Defendants' implied promises to Plaintiffs and Class members include, but are not

limited to: (1) taking steps to ensure that anyone who is granted access to PII also protects the confidentiality of that data; (2) taking steps to ensure that the PII placed in control of Defendants' employees is restricted and limited only to achieve authorized business purposes; (3) restricting access to employees and/or agents who are qualified and trained; (4) designing and implementing appropriate retention policies to protect PII; (5) applying or requiring proper encryption and/or the separation of different data sets; (6) implementing multifactor authentication for access; and (7) taking other steps to protected against foreseeable breaches.

102. Plaintiffs and Class members would not have entrusted their PII to Defendants in the absence of such an implied contract.

103. Defendants violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class members' PII.

104. Plaintiffs and Class members have been damaged by Defendants' conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein. Plaintiffs seek damages, including restitution, actual damages, nominal damages, and any other awardable form of damages, in an amount to be proven at trial.

COUNT III

UNJUST ENRICHMENT

105. Plaintiffs repeat and reallege all preceding paragraphs as if fully set forth herein.

106. This count is asserted in the alternative to breach of implied contract (Count II).

107. Plaintiffs and Class members conferred a benefit on Defendants with their money and data. Specifically, they purchased services from Coinbase and, in so doing, also provided Defendants with their PII. In exchange, Plaintiffs and Class members should have received from

Defendants the services that were the subject of the transaction and should have had their PII been protected with adequate data security.

108. Defendants knew that Plaintiffs and Class members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the PII of Plaintiffs and Class members for business purposes.

109. In particular, Defendants enriched themselves by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to increase their own profits at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures. Plaintiffs and Class members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize their own profits over the requisite security.

110. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Class members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

111. Defendants failed to secure Plaintiffs' and Class members' PII and, therefore, did not provide full compensation for the benefit Plaintiffs and Class members provided.

112. Defendants acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

113. Had Plaintiffs and Class members known that Defendants had not reasonably secured their PII, they would not have agreed to provide their PII to Defendants.

114. Plaintiffs and Class members have no adequate remedy at law.

115. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their PII is used; (c) the compromise, publication, and/or theft of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect PII in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class members.

116. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm.

117. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that Defendants unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Coinbase's services.

VI. PRAYER FOR RELIEF

118. WHEREFORE, Plaintiffs, on their own behalf and on behalf of all others similarly situated, pray for relief as follows:

- A. For an Order certifying this case as a class action and appointing Plaintiffs and their counsel to represent the Class;
- B. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;
- C. For injunctive and other equitable relief to ensure the protection of the sensitive information of Plaintiffs and the Class which remains in Defendants' possession;
- D. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- E. Pre- and post-judgment interest on any amounts awarded; and
- F. Such other and further relief as the Court may deem just and proper.

VII. JURY TRIAL DEMAND

119. Plaintiffs hereby demand a trial by jury on all claims so triable.

DATED: May 15, 2025

Respectfully submitted,

/s/ Israel David

Israel David
israel.david@davidllc.com
Adam. M. Harris
adam.harris@davidllc.com
ISRAEL DAVID LLC
60 Broad Street, Suite 2900
New York, New York 10004
Telephone: (212) 350-8850

Attorneys for Plaintiffs and the Proposed Class